EXPREES MAIL ED 045469955 US

Navy Case No. 82100

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Christian L. Houlberg and Gary S.Borgen

Application No.: 09/505,830 Group No.: 2135

Filed: February 17, 2000 Examiner: James Seal

For: NON-VOLATILE MEMORY FOR USE WITH AN ENCRYPTION DEVICE

Mail Stop Appeal Briefs-Patents
Commissioner For Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPELLANT'S BRIEF (37 C.F.R. § 1.192)

Sir:

This brief is in furtherance of the Notice of Appeal, filed in this case on May 28, 2004.

1. REAL PARTY IN INTEREST

The real party of interest in the above entitled application is the United States of America as represented by the Secretary of the Navy as assignee of the entire interest in the subject invention of the above named inventors.

2. RELATED APPEALS AND INTERFERENCES

There are no prior appeals or interferences related to this appeal.

3. STATUS OF CLAIMS

A. TOTAL NUMBER OF CLAIMS IN APPLICATION.

There are sixteen claims in the application.

B. STATUS OF ALL CLAIMS

1. Claims cancelled: Claims 1-12, 14 and 15.

2. Claims pending: Claims 13 and 16. Claims 13 and 16 stand finally rejected under 37 C.F.R 103(a).

A correct copy of claims 13 and 16 on appeal appears in the accompanying APPENDIX.

4. STATUS OF AMENDMENTS

An amendment under 37 C.F.R. 1.116 is being submitted with this appeal brief canceling claims 6-12. This amendment is being submitted within the three month shortened statutory period for reply from the final Office action of May 21, 2004. The Examiner has not acted upon the amendment.

5. SUMMARY OF INVENTION

A concise explanation of the subject invention covered by the claims on appeal is as follows:

The present invention relates to a Non-Volatile Memory circuit for use with a missile's telemetry encryption system.

Referring to FIGS. 1 and 2 (page 4, line 22 thru page 5, line 12), the missile's telemetry system includes a key loader (22) for loading a crypto key with its corresponding check word into a Non-Volatile Memory circuit (20). The Non-Volatile Memory circuit (20) is connected to an encryption device (24) which allows Non-Volatile Memory circuit (20) to load a crypto key with its corresponding check word into the encryption device (24). The encryption device (24) is connected to a telemeter transmitter (26) which transmits encrypted telemetry data from the encryption device (24) to a ground station.

Referring to FIG. 2 (page 5, lines 13-20), Non-Volatile Memory circuit (20) functions as an interface between key loader (22) and encryption device (24). Included in the Non-Volatile Memory circuit (20) is an 8-bit Microcontroller (32) which has a non-volatile EEPROM suitable for storage of a crypto key and its corresponding checkword and also a backup crypto key and checkword.

Referring to FIG. 2, a pair of light emitting diodes (36 and 38) are also connected to the microcontroller (32) to indicate the status of a load of the crypto key and checkword within the microcontroller (32) (page 11, lines 15-20) as well as the status of an erase of the crypto key and checkword from the microcontroller (32) (page 7, lines 10-19).

Referring to FIGS. 1 and 2 (page 10, line 1 thru page 11, line 15), the microcontroller (32) is also connected to the telemeter transmitter (26) for the missile. This allows the microcontroller (32) to turn off the transmitter (26) during a key load of the encryption device (26) which prevents transmission by telemeter transmitter (26) of the crypto key and its corresponding checkword. When the encryption device (26) is successfully loaded, the software within the microcontroller (32) enables the telemeter transmitter (26).

Referring to FIGS. 1 and 2 (page 12, line 1 thru page 13, line 1), when the microcontroller (32) completes a down load of the crypto key from its internal EEPROM to the encryption device (26) and upon launch of the missile, the software within the microcontroller (32) erases the crypto key and its corresponding checkword from its EEPROM. This prevents an enemy force from retrieving the crypto key and its corresponding checkword from the missile after launch. The microcontroller (32) can also erase the crypto key and its corresponding checkword from its EEPROM upon receiving an active erase signal from the missile.

The computer software for the microcontroller (32) is illustrated in the flow charts of FIGS. 4 and 9. Specifically, the flow chart of FIG. 4 illustrates the main routine for the computer software used by microcontroller (32).

During program step 44 of FIG. 4, the software test for the presence of the key loader (22). When the SENSE_IN line is high resulting in a "1" at the RA0 input of the microcontroller (32), the software proceeds to the eeprom_key_load routine of FIG. 6.

During program step 70 of FIG. 6, the transmitter (26) is disabled by microcontroller 32 to prevent possible transmission of the crypto key and checkword. During program step 74 of FIG. 6, the checkword is loaded into the EEPROM of microcontroller (32). The crypto key is be transferred from the key loader (22) to the EEPROM of the microcontroller (32) during program step 80 of FIG. 6, with the key being loaded into the EEPROM of micrcontroller (32) during program step 82 of FIG. 6.

Program step 84 of FIG. 6, provides an indication the crypto key is present by turning off the erase LED (38). During program step 86, the transmitter (26) is enabled by the software of microcontroller (32).

When the crypto key is correctly loaded into the EEPROM of micrcontroller (32), the software for microcontroller (32) proceeds to program step 50 of FIG. 4 which is the KGV encryption unit load attempt decision. When a decision is made to load the encryption device (24), the software for microcontroller (32) proceeds to the routine kgv_key_load which is illustrated in FIG. 7.

During program step 90 of FIG. 7 (page 8, lines 11-18), transmitter (26) is disabled. During program step 92 of FIG. 7, the KGV-68 encryption device's sense input (ENCR_SENSE_IN input to the encryption device 24) is set active to start a load of the crypto key with its corresponding check word.

Encryption device (24) then responses with an active low variable request signal (/ENCR_VAR_RQ output of the encryption unit) to microcontroller (32) which occurs during program step 94 of FIG. 7 (page 10, lines 5-7). During program step 100 of FIG. 7, there is an indication within micrcontroller (32) that the key should be present. During program step (102) a wait routine occurs within microcontroller (32) which allows for completion of the key load process. When the key load process is complete, the KGV sense input (ENCR_SENSE_IN input to the encryption device)) is set inactive to a logic "zero" state (program step 104 of FIG. 7, page 10, lines 12-19).

When the crypto key and checkword are successfully loaded into the encryption device (24), transmitter (26) is enabled (program step 114 of FIG. 7). When this occurs the status light emitting diode (36) will remain on (program step 116 of FIG. 7) to indicate that microcontroller (32) has been successful in its attempt to load the encryption device (24) (page 11, lines 14-20).

The routine for erasing the EEPROM within microcontroller (32) is erase_key routine of FIG. 8, which is entered via program step 54 of FIG. 4. Whenever the signal provided to the RA4 input to the microcontroller (32) is a logic "one", the software proceeds to program step 124 of FIG. 8 erasing the crypto key with its corresponding check word from the EEPROM within microcontroller (32). The erase light emitting diode (38) is set, and the load status is displayed during program step 124 of FIG. 8 (page 12, lines 16-24 and page 13, line 1).

6. ISSUES

Presented for review in this appeal is a final rejection under 35 U.S.C. 103(a), involving the following issues:

Whether claims 13 and 16 are unpatentable over the prior art references Borgen H1414, in view of Maher 5,513,261, Best 4,465,901 and Wade 98/07099, which are relied upon by the Examiner.

7. GROUPING OF CLAIMS

Claims 13 and 16 form a group of claims related to an apparatus for providing a crypto key and an associated checkword of the crypto key to an encryption device for the telemetry system of a missile.

8. ARGUMENT

ARGUMENT UNDER 35 U.S.C § 103

It is respectfully submitted that the combination of the reference teachings of Borgen H1414, in view of Maher 5,513,261, Best 4,465,901, and Wade, 98/07099 as proposed by the Examiner in the office action of May 21, 2004 would not have resulted in the invention recited in the claims.

Claim 13 recites a microcontroller (32) as including an internal EEPROM for storing the crypto key and the associated checkword and a copy of the crypto key and the associated checkword (lines 15-18 of claim 13).

Claim 13 also recites the microcontroller (32) as containing a computer software program for controlling, handling and interpreting the transfer and loading of the crypto key and associated checkword from the key loader (22) into encryption device (24) (lines 54-79 of claim 13).

Specifically, claim 13 recites a computer software program which controls, handles and interprets the transfer of the crypto key and checkword from the key loader (22) to microcontroller (32) and the storage of the crypto key and checkword within the EEPROM of microcontroller (32) in the manner depicted in the flow charts of FIGS. 4, 5 and 6. Further, claim 13 recites the computer software program as controlling, handling and

interpreting the loading of the crypto key and checkword into the encryption device (24) as depicted in FIGS. 4 and 7 and the disabling of transmitter (26) during the loading process which is program step 90 of FIG. 7. Claim 13 also recites the enabling of transmitter (26) after a successful load of the crypto key and checkword, which is program steps 110 and 114 of FIG. 7.

Borgen teaches a sequencing control circuit 75 connected to an external EPROM 332 and a static RAM 78. The sequencing control circuit 75 is connected to the power control circuit 41 and the RAM interface circuit 76 of Fig. 1A. The external EPROM 332 is also connected to the power control circuit 41 and the RAM interface circuit 76 of Fig. 1A.

Static RAM 78 receives and stores a key word from a loader 276. Sequencing control circuit 75 provides logic signals for controlling read and write operations of static RAM 78, as well as logic signals to allow for transfer or down loading of the key word from the loader 276 to the static RAM 78.

Borgen also teaches sequencing control circuit 75 as providing logic signals to interface with an encryption device 286 which allows the key word to be transferred or up loaded from the static RAM 78 to the encryption device 288.

The EEPROM 332 of Borgen provides program instructions which control the sequence of operation within the nonvolatile memory

system including static RAM 78. Addressing for the EEPROM 332 is provided by sequencing control circuit 75.

The digital hardware/digital logic circuitry for sequencing control circuit 75 is depicted in detail in FIG. 10. The digital logic circuitry of FIG. 10 includes ten bit parallel loadable up counter 140, four eight bit latches 180, 206, 208, and 210, control circuit 168, eight by two bit comparator 250, eight-to-one multiplexer circuit 262, Johnson counter 110, eight bit binary counter 230, eleven bit binary counter 182, and four-to-one demultiplexer 334.

Further, the control circuit 168 for sequencing control circuit 75 includes the 26 logic gates illustrated in Figs. 23A-23F.

The entire non-volatile memory system disclosed in Borgen includes the numerous logic elements illustrated in Figs. 1A (29 logic elements), Fig. 11 (12 logic elements comprising Johnson counter 110), Fig. 13 (20 logic elements comprising counter 140), Fig. 16 (11 logic elements comprising counter 182), Fig. 14 (5 logic elements comprising each of the ten load circuits 162 in Fig. 13), Fig. 17 (8 logic elements comprising each of the latches 180, 206, 208 and 210 of Fig. 10), Fig. 18 (8 logic elements comprising multiplexer circuit 262 of Fig. 10), Fig. 19 (the eight one bit comparator circuits 252 which make up

comparator 250 of Fig. 10), Fig. 21 (the logic elements which make up multiplexer circuit 262), Fig. 23A-23F (26 logic elements which make up control circuit 168 of Fig. 10), and Fig. 31 (the logic elements which make up demultiplexer 334 of Fig. 10).

Except for the EEPROM 332 and the static RAM 78, the nonvolatile memory system of Borgen is made of NAND gates, NOR gates, inverters, flip-flops, buffer gates, transmission gates 364-398, transmission gates 340-354 and a binary counter 40 which are basic logic elements used in the design of the numerous logic circuits disclosed in Borgen.

The present invention accomplishes the function of Borgen, but eliminates the need for the extremely complex hard wired logic circuitry of Borgen by replacing the logic circuitry with a microprocessor which generate all the logic signals needed to transfer, store and then load the crypto key and checkword into the encryption device using the computer software program illustrated in FIGS. 4-9, program steps 40-156, and claimed in claim 13. Further, there is no teaching in Borgen of transferring and then loading an associated checkword into the encryption device, although the Examiner asserts this would be obvious in view Maher.

Applicants, however, must respectfully disagree since the hard wired logic circuit design of Borgen would necessitate added

logic circuitry which more than likely would be as complex or more complex than logic circuitry for the sequencing control circuit 75. It needs to be understood that any change in the function of sequencing control circuit 75 requires a substantial change in the hard wired digital logic circuitry of sequencing control circuit 75, a complex electronic design change which applicants respectfully submit is not obvious in view of the teachings of Borgen in view of Maher.

The Examiner now suggest that the microcontroller 10 of Wade in combination with Borgen and Maher would motivate one of ordinary skill in the art at the time the invention was made to replace the external memory, I/O, sequencing control and other circuitry of the Borgen Circuit with a monolithic microcontroller having internal memory. The Examiner reasons that the lower fabrication cost and higher reliability of the microcontroller of Wade and the better security of the internal memory would provide the motivation to replace the external memory, I/O, sequencing control circuitry of Borgen with the microcontroller of Wade.

Applicants respectfully disagree with this assertion by the Examiner. Wade teaches a microcontroller 10 having an internal memory array 34 which preferably includes high-density dynamic random access (DRAM) memory cells. Alternately, Wade teaches the memory array as including lower density static random access

(SRAM) memory cells. DRAM memory cells and SPRAM memory are volatile memory devices which require an external power source, e.g. a battery, to store information for lengthy periods of time.

The invention recited in claim 13 includes the microcontroller with internal EEPROM for storing the crypto key and checkword. The applicants selected the 18-pin Flash/EEPROM 8-bit microcontroller, used in the preferred embodiment because the microcontroller's internal EEPROM memory is a non-volatile memory which stores data for lengthy periods of time without the need for a backup battery or other power source. Since missiles are often stored for years before use there is need to insure that the encryption data remains in tact until the missile is deployed. The microcontroller's volatile DRAM or SRAM memory suggested by Wade would not work in the applicants' claimed invention as recited in claim 13.

It is respectfully submitted that the required teaching, or suggestion to combine the references as proposed by the Examiner to render the invention of claim 13 obvious is not present since the cited prior art either individually or in combination does not teach the use of a micrcontroller with an internal non-volatile memory.

It is further submitted that Wade teaches away from the invention of claim 13 in that memory cell 34 preferably includes

DRAM memory cells which require additional refresh circuitry to provide periodic memory cell refreshing.

In re Hedges, 783 F.2d 1038, 228 USPQ 685 (Fed Cir. 1986) is illustrative of the concept of "teaching away" as supporting a finding of nonobviousness of the claimed invention by the Court of Appeals for the Federal Circuit (CAFC). Hedges had stressed to the Patent and Trademark Office that his invention incorporated a reaction of diphenyl sulfone at a temperature above its melting point of 127 degrees centigrade. Hedges argued that the low temperatures shown by the prior art defeat any prima facia case of obviousness. The PTO disagreed stating that the references defined a prima facia case of obviousness.

Judge Newman of the CAFC wrote that the invention was not obvious over the prior art noting that the references all suggest that lower temperatures of reaction are preferable and that Hedges proceeded contrary to the accepted wisdom.

Applicants in making their invention realized the need for a nonvolatile EEPROM for long term storage of the crypto key and checkword, which was contrary to the accepted wisdom at the time of the making of the invention as is evidenced by the teaching of Wade at page 7, lines 20-24, wherein it is clearly stated that:

> Memory array 34 perferably includes many high-density dynamic random access memory (DRAM) memory cells. In this

case, memory control unit 32 also perferably includes refresh circuitry to provide periodic memory cell refreshing. Alternatively, memory array 34 may include many lower density static random access memory (SRAM) memory cells.

Thus, based on the above teaching of Wade and the CAFC holding in *In re Hedges, supra,* it is respectfully submitted the Examiner's proposed combination is not sufficient to establish a prima facia obviousness rejection.

The Examiner admits that the cited references are silent on disabling the transmitter circuitry while down loading the crypto key. To overcome this lack of a teaching in the prior art, the Examiner argues that one of ordinary skill in the art would have been motivated to disable any transmitter to provide for accidental transmission of the key material leading to compromises of data and certainly would be TEMPEST noncompliant.

Claim 13 recites an 8-bit microcontroller which includes a computer software program for controlling the downloading and transfer of the crypto key and associated checkword from the loader 22, the storage of the crypto key and checkword in the EEPROM of microcontroller 32 and the loading of the crypto key and checkword into the encryption device 24. In addition, the claim recites the transmitter 26 as being disabled during the

loading process and being enabled after a successful load of crypto key and checkword into the encryption device 24.

The above recited limitations are not disclosed, taught or even suggested by the prior art Borgen SIR or any of the cited references as admitted by the Examiner. The teaching of Borgen is a hard wired logic circuit which is very complex, includes hundreds of logic gates and is capable of performing only one function, the transfer and temporary storage of a key word into the static RAM 78 and the subsequent loading of the key word into the encryption circuit 288. The present invention performs this function and additional functions set forth in the previous paragraph through the use of the computer software program of Figs. 4-9 and microcontroller 32 with its internal EEPROM. This is definitely not the teaching of Borgen which teaches only a hard wired digital logic circuit capable of performing the single function of transferring the key word from the loader to the static RAM and then to the encryption device. The remaining cited prior art also fails to even suggest the disabling of the transmitter during a crypto key load

The Federal Circuit has stated that a prima facia case of obviousness requires that the references generally place the needed subject matter supporting the obviousness rejection in the public domain before the date of the invention. See, for

example, *In re Zenitz*, 333 F.2d 924, 142 USPQ 158, 160 (C.C.P.A. 1964). The court in *Zenitz, supra,* stated at 142 USPQ 160 that:

> The question is not what the applicant is aware at the time he made the invention, but whether his invention would be obvious in view state of the art at the time it was made.

The Examiner uses the phrase "TEMPEST noncompliance" to support his position that the claimed recitation of turning off the transmitter during a key load is in the public domain.

Tempest information, that is information relating to encryption of data, especially with respect to weapons systems is almost always classified by the military. Thus such information is not in the public domain. The applicants are employed by the Navy to design communications and telemetry equipment for military weapons systems such as missiles. The applicants were aware of the requirement to turn off the transmitter during the crypto key load process. However, the state of the art, is such that this information is not in the public domain because of classification issues and is thus not available to one of ordinary skill in the art. Evidence to support this position is the Examiner's inability to find a reference which supports the Examiner's contention that turning of the transmitter during the key load is well within the purview of one of ordinary skill in the art.

Claim 13 also recites light emitting diodes 36 and 38 for providing status of the load and erase functions controlled by the microcontroller's software as illustrated in Figs. 4-9.

Specifically, Claim 13 recites light emitting diode 36 as displaying the status for the load of the crypto key and associated checkword into the encryption device and light emitting diode 38 as displaying the status of an erase of the crypto key and checkword from the 8-bit microcontroller. Borgen does not provide a teaching or even a suggestion as to these claim limitations. As with each of the other limitations which Borgen fails to disclose or even suggest, this limitation, i.e. adding status LEDs 36 and 38 for the load and erase functions would require additional digital logic circuitry to implement the claimed limitation.

Applicants' invention implements these functions through the microcontroller's software as recited in claim 13.

The Examiner states that it would have been obvious because the use of a low power LED as a visual indicator of the success of a download of the key material into the encryption device before telemetry was transmitted would lessen the likelihood of compromise of classified material. The Examiner, however, admits that the prior art is silent as to whether status information about the download of the key is displayed.

The Examiner also admits that the prior art is silent with regards to the erase of the key and checkword from the EEPROM memory but the Examiner argues that it have been obvious to use an LED indicator light as a visual means to determine if previous key material were erased to prevent detection of the material.

The Federal Circuit has stated that "[o]bviousness cannot be established by combining the teachings of the prior art to produce the claimed invention, absent some teaching, suggestion or incentive supporting the combination. See *In re Geiger*, 815 F.2d 686, 2 USPQ 2d 1276, 1278 (Fed. Cir. 1987).

In *W.L. Gore & Associates, Inc. v. Garlock, Inc.*, 721 F.2d 1540, 220 USPQ 303, 311 (Fed. Cir. 1983), Chief Judge Markey, in his opinion for the CAFC (Court of Appeals, Federal Circuit) stated:

> In concluding that obviousness was established by the teachings in various pairs of references, the district court lost sight of the principle that there must have been something present in those teachings to suggest to one skilled in the art that the claimed invention before the court would have been obvious.

With respect to the first and second light emitting diode recited, respectively at lines 37-40 and lines 49-53 of claim 13, the Examiner has admitted that the prior art Borgen, Maher, Best

and Wade patents are silent, that is the prior art fails to provide the necessary teaching to suggest to one skilled in the art that the claimed invention is obvious. The Examiner appears to have relied on assumptions that have no evidentiary support in the prior art to establish his prima facia case of obviousness.

As in *W.L. Gore & Associates, Inc. v. Garlock, Inc., supra,* there is simply no teaching in the cited art as to the need for providing status information by visual indicators (light emitting diodes 36 and 38) to suggest to one of ordinary skill in the art that the claimed invention is obvious. Thus, it is respectfully submitted that the absence of these teachings is very strong evidence of the nonobviousness of the claimed invention.

The Examiner asserts that the software programs for controlling, handling and interpreting the transfer of the key material from the key loader to the internal EEPROM and then to the encryptor, testing and finally enabling the transmitter after successfully loading the encryptor is a software of the apparatus and the same prior art applies to the software implementation.

The microprocessor applicants selected for use in their invention includes a counter timer. The counter timer is critical in the transfer of the crypto key and checkword from the microcontroller 32 to the encryption device 24.

Specifically, signal timing and pulse width shaping are

critical to a successful load of the key and checkword into the encryption device 24. For example, the KGV-68 encryption device 24 requires the clock signal supplied to the encryption device to have a time period T (FIG. 3C) of between 100 ns and 20 ms. The counter timer in microcontroller 32 insures that the clock signal has a time period T within this range. Further, there are timing requirements which must be met to insure that the status light emitting diodes 36 and 38 are operating correctly.

The timer counter also allows for multiple operations to occur simultaneously. For example, the microcontroller controls the status light emitting diodes 36 and 38 while monitoring the data lines and other signal lines to the encryption device 32 to insure a successful load of the key and checkword into the encryption device 32.

The prior art Wade publication discloses a micrcontroller which does not have a timer counter. The Wade microcontroller has a structure similar to Intel's 80186 and 80188 micrcontrollers. For example, the disclosure of Wade states at page 8, lines 7-8 that the embodiment of EMAR 38 is similar to the PCS and MCS auxiliary register of 80186 and 80188 micrcontrollers. The Intel data sheet for their i486™ Microprocessors series illustrate the 486 Microprocessor Pipelined 32-Bit Microarchitecture, a copy of which is being

submitted with the brief as Exhibit A. Exhibit A fails to disclose or even suggest a counter timer within the microarchitecture for the i486™ microprocessor.

The CCPA and the Federal Circuit have consistently held that whenever a reference requires some modification to meet the claimed invention and the modification destroys the purpose or function of the invention, one of ordinary skill in the art would not have found a reason to make the claimed modification.

An excellent example of such an evaluation is in *In re Gorden*, 737 F.2d 900, 221 USPQ 1125 (Fed.Cir. 1984) which involved a blood filter assembly used during surgery and other medical procedures. In operation, blood would enter the bottom of the device, move along a spirally upward path through a filter, and then be let out at the bottom of the assembly. With the blood inlet at the bottom end, gas bubbles would rise upwardly out of the blood, facilitating their removal.

The prior art was a patent to French (U.S. Patent No. 1,175,948) that disclosed a liquid strainer for removing dirt and water from gasoline and other light oils. In contrast to the claimed blood filter assembly, the inlet and outlet in the French device were located at the top, whereby gravity assisted in the separation of heavier oils and water. The court in rejecting the PTO's assertion that the claimed invention was obvious in view of

the French patent noted that if the French device were turned upside down it would be rendered inoperable for its intended purpose because gasoline to be filtered would then be trapped, the water sought to be separated would flow freely out, and unwanted dirt would build up.

The Examiner's proposed modification of Borgen using the microcontroller of Wade would destroy the purpose or function of the invention. Since the microcontroller of the Examiner's proposed combination does not include a timer counter, the proposed combination would not be able to execute a successful transfer and load of the key and checkword into encryption device 24 for the reasons set forth above which include control signal timing, and multiple function capability.

Thus, it is respectfully submitted that the proposed modification of Borgen to include the Wade micrcontroller and software is not proper and the prima facia case of obviousness can not be made.

With respect to the limitation of claim 16, claim 16 is dependent from claim 13 which it is submitted is in condition for allowance and is thus allowable for the reasons set forth above.

The lack of any teaching or suggestion in the prior art as to (1) the status light emitting diodes and (2) the microprocessor's function of turning off the transmitter during a

key load provides very strong evidentiary support for the applicants position that the claimed inventions are not obvious. Additional support is found in the "teaching away" of Wade as to the use of volatile memory and a refresh circuit in the preferred embodiment and the lack of a counter timer in the microprocessor of Wade which renders the Examiner's proposed combination inoperative. Further, since the hard wired logic of Borgen is being replaced with computer software which performs the functions of Borgen and additional functions it is very difficult if not impossible to imagine that one of ordinary skill in the art given the Examiner's proposed combination could make the Applicants claimed invention. The required teachings to establish a prima facia case are not present in the prior art of record.

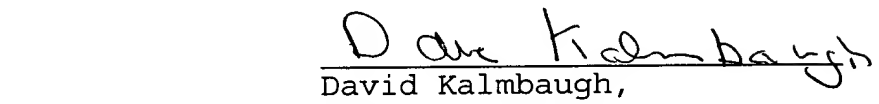
On the entire record and in view of all the references, each in its entirety, it is clear that one of ordinary skill in the art at the time the invention was made would not have found a reason to make the invention in the manner proposed by the Examiner.

CONCLUSION

In view of the foregoing, reversal of the final rejection of claims 13 and 16 on appeal under 35 U.S.C. 103(a), as stated in

the final Office action, is believed to be in order and allowance of claims 13 and 16 is respectfully requested.

Respectfully submitted,



David Kalmbaugh,
Reg. No. 29,234

Attachments: Exhibit A

Tele: (805) 989-8266

Office of Counsel, Code K00000E
NAVAIR WEAPONS DIVISION
575 "I" AVENUE, SUITE ONE
POINT MUGU, CA 93042-5049

9. APPENDIX

Claims 13 and 16 are as follows:

13. An apparatus for providing a crypto key and an associated checkword of said crypto key to an encryption device for a telemeter system of a missile, said apparatus comprising:

a key loader having said crypto key and said associated checkword stored therein;

an 8-bit microcontroller connected to said key loader to receive said crypto key and said associated checkword from said key loader, said 8-bit microcontroller sending a first variable request signal to said key loader to effect a transfer of said crypto key and said associated checkword from said key loader to said 8-bit microcontroller for storage within said 8-bit microcontroller;

said 8-bit microcontroller including an internal EEPROM for storing said crypto key and said associated checkword and a copy of said crypto key and said associated checkword;

said 8-bit microcontroller being connected to said encryption device, said 8-bit microcontroller sending a sense in signal to said encryption device to initiate a load of said crypto key and said associated checkword

into said encryption device;

said 8-bit microcontroller receiving from said encryption device a second variable request signal, said 8-bit microcontroller, responsive to said second variable request, loading said crypto key and said associated checkword into said encryption device;

said 8-bit microcontroller being connected to a transmitter for the telemeter system of said missile, said 8-bit microcontroller providing a transmitter disable signal to said transmitter to disable said transmitter when said crypto key and said associated checkword are loaded into said encryption device preventing said crypto key and said associated checkword from being transmitted by said transmitter;

a first light emitting diode connected to said 8-bit microcontroller, said first light emitting diode displaying a status for a load of said crypto key and said associated checkword into said encryption device;

said 8-bit microcontroller being connected to a missile interface within said missile to receive a launch signal from said missile interface upon a launch of said missile, said 8-bit microcontroller, responsive to said launch signal, erasing said crypto key and said

associated checkword and the copy of said crypto key and said associated checkword from the internal EEPROM of said 8-bit microcontroller;

a second light emitting diode connected to said 8-bit microcontroller, said second light emitting diode displaying a status for an erase of said crypto key and said associated checkword from said 8-bit microcontroller; and

said 8-bit microcontroller containing a computer software program for controlling, handling and interpreting said transfer of said crypto key and said associated checkword from said key loader to said 8-bit microcontroller for storage within the internal EEPROM of said 8-bit microcontroller, said computer software program controlling, handling and interpreting the storing of said crypto key and said associated checkword and said copy of said crypto key and said associated checkword within the internal EEPROM of said 8-bit microcontroller, said computer software program controlling, handling and interpreting the loading of said crypto key and said associated checkword into said encryption device from the internal EEPROM of said encryption device, said computer software program

controlling, handling and interpreting a disabling of said transmitter when said crypto key and said associated checkword are loaded into said encryption device and an enabling of said transmitter after a successful load of said crypto key and said associated checkword into said encryption device, and said computer software program controlling, handling and interpreting the erasing of said crypto key and said associated checkword and the copy of said crypto key and the associated checkword from the internal EEPROM of said 8-bit microcontroller.

16. The apparatus of claim 13 wherein said 8-bit microcontroller is connected to a loader interface within said missile to receive an erase signal from said loader interface, said 8-bit microcontroller, responsive to said erase signal, erasing said crypto key and said associated checkword and the copy of said crypto key and the associated checkword from the EEPROM of said 8-bit microcontroller.

EXHIBIT A

SERIAL NO. 09/505,830
FILING DATE: 02/17/200
INVENTORS: CHRISTIAN HOULBERG AND GARY BORGEN
FOR: NON-VOLATILE MEMORY FOR USE WITH AN ENCRYPTION DEVICE

intel®

i486™ MICROPROCESSOR

- **Binary Compatible with Large Software Base**
  - **MS-DOS*, OS/2**, Windows**
  - **UNIX*** System V/386**
  - **iRMX®, iRMK™ Kernels**
- **High Integration Enables On-Chip**
  - **8 Kbyte Code and Data Cache**
  - **Floating Point Unit**
  - **Paged, Virtual Memory Management**
- **Easy To Use**
  - **Built-In Self Test**
  - **Hardware Debugging Support**
  - **Intel Software Support**
  - **Extensive Third Party Software Support**
- **168-Pin Grid Array Package**
- **High Performance Design**
  - **Frequent Instructions Execute in One Clock**
  - **25 MHz and 33 MHz Clock Frequencies**
  - **80 and 106 Mbyte/Sec Burst Bus**
  - **CHMOS IV Process Technology**
  - **Dynamic Bus Sizing for 8-, 16- and 32-Bit Busses**
- **Complete 32-Bit Architecture**
  - **Address and Data Busses**
  - **Registers**
  - **8-, 16- and 32-Bit Data Types**
- **Multiprocessor Support**
  - **Multiprocessor Instructions**
  - **Cache Consistency Protocols**
  - **Support for Second Level Cache**

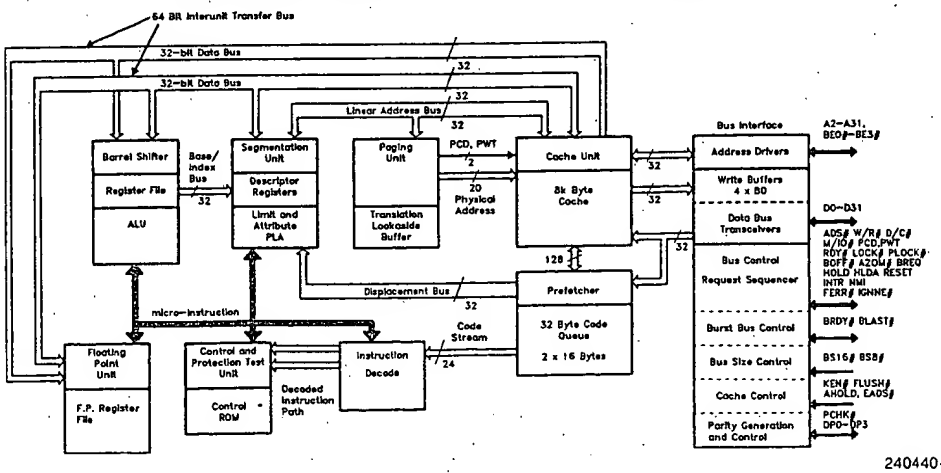
The i486™ CPU offers the highest performance for DOS, OS/2, Windows and UNIX System V/386 applications. It is 100% binary compatible with the 386™ CPU. Over one million transistors integrate cache memory, floating point hardware and memory management on-chip while retaining binary compatibility with previous members of the X86 architectural family. Frequently used instructions execute in one cycle resulting in RISC performance levels. An 8 Kbyte unified code and data cache combined with a 106 Mbyte/Sec burst bus at 33.3 MHz ensure high system throughput even with inexpensive DRAMs.

New features enhance multiprocessing systems. New instructions speed manipulation of memory based semaphores. On-chip hardware ensures cache consistency and provides hooks for multilevel caches.

The built in self test extensively tests on-chip logic, cache memory and the on-chip paging translation cache. Debug features include breakpoint traps on code execution and data accesses.

5

i486™ Microprocessor Pipelined 32-Bit Microarchitecture



240440-1

iRMX, iRMK, 386, 387, 486, i486 are trademarks of Intel Corporation.
*MS-DOS® is a registered trademark of Microsoft Corporation.
**OS/2™ is a trademark of Microsoft Corporation.
***UNIX™ is a trademark of AT&T.

November 1990
Order Number: 240440-003